CLAIMS

What is claimed is:

1. In a video source device, a method comprising:

a video source application requesting from a video hardware interface status with respect to a link linking said video source device to an external video sink device, and supplementing said status request with a first basis value to a symmetric ciphering/deciphering process;

the video source application receiving from said video hardware interface said requested status and a verification key, generated through said symmetric ciphering/deciphering process employing said first basis value; and

the video source application verifying the correctness of said verification key to determine whether to trust said provided status.

2. The method of claim 1, wherein said method further comprises said video source application supplementing said status request with a selection key for the video hardware interface to use to generate an authentication key for use to generate said verification key.

3. The method of claim 1, wherein said verification of the correctness of the received verification key comprises said video source application independently generating its own copy of the verification key.

4. The method of claim 3, wherein said independent generation of said video source application's own copy of said verification key comprises said video source

application independently generating its own copy of an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

5. The method of claim 3, wherein said independent generation of said video source application's own copy of said verification key comprises said video source application applying a one way function to at least a first selected subset of said first basis value provided to said video hardware interface using an independently generated copy of an authentication key.

6. The method of claim 5, wherein said independent generation of said video source application's own copy of said verification key further comprises said video source application applying said one way function to a selection key said video hardware interface received from said video sink device for use by said video hardware interface to authenticate said video sink device, using the result of said first application of the one-way function.

7. The method of claim 6, wherein said independent generation of said video source application's own copy of said verification key further comprises said video source application applying said one way function to at least a second selected subset of said first basis value provided to said video hardware interface using the result of said second application of the one-way function.

8. The method of claim 6, wherein said independent generation of said video source application's own copy of said verification key further comprises said video

source application applying said one way function to at least said status using the result of said second application of the one-way function.

9. The method of claim 1, wherein said method further comprises

said video source application requesting from said video hardware interface a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to said external video sink device, and supplementing said secret request with a second basis value to said symmetric ciphering/deciphering process;

the video source application receiving from said video hardware interface said requested secret in a ciphered form, having been ciphered with a ciphering key generated using said symmetric ciphering/deciphering process and employing said second basis value; and

the video source application deciphering said ciphered secret using an independently generated copy of said ciphering key.

10. The method of claim 9, wherein said method further comprises said video source application supplementing said secret request with a selection key for the video hardware interface to use to generate an authentication key for use by said symmetric ciphering/deciphering process.

11. The method of claim 9, wherein said method further comprises said video source application independently generating its own copy of the ciphering key.

12. The method of claim 11, wherein said independent generation of said video source application's own copy of said ciphering key comprises said video source

application independently generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

13. The method of claim 11, wherein said independent generation of said video source application's own copy of said ciphering key comprises said video source application applying a one way function to at least a first selected subset of said second basis value provided to said video hardware interface using an independently generated copy of an authentication key.

14. The method of claim 13, wherein said independent generation of said video source application's own copy of said ciphering key further comprises said video source application applying said one way function to at least a second selected subset of said second basis value provided to said video hardware interface using the result of said first application of the one-way function.

15. In a video source device, a method comprising:

a video source application requesting from a video hardware interface a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to an external video sink device, and supplementing said secret request with a basis value to said symmetric ciphering/deciphering process;

the video source application receiving from said video hardware interface said requested secret in a ciphered form, having been ciphered using a ciphering key generated using said symmetric ciphering/deciphering process and employing said basis value; and

the video source application deciphering said ciphered secret using an independently generated copy of said ciphering key.

16. The method of claim 15, wherein said method further comprises said video source application supplementing said secret request with a selection key for the video hardware interface to use to generate an authentication key for use by said symmetric ciphering/deciphering process.

17. The method of claim 15, wherein said method further comprises said video source application independently generating its own copy of the ciphering key.

18. The method of claim 17, wherein said independent generation of said video source application's own copy of said ciphering key comprises said video source application independently generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

19. The method of claim 17, wherein said independent generation of said video source application's own copy of said ciphering key comprises said video source application applying a one way function to at least a first selected subset of said basis value provided to said video hardware interface using an independently generated copy of an authentication key.

20. The method of claim 19, wherein said independent generation of said video source application's own copy of said ciphering key further comprises said video source application applying said one way function to at least a second selected

subset of said basis value provided to said video hardware interface using the result of said first application of the one-way function.

21. In a video source device, a method comprising:

a video hardware interface receiving from a video source application a request for status with respect to a link linking said video source device to an external video sink device, and said status request being supplemented with a first basis value to a symmetric ciphering/deciphering process;

the video hardware interface returning said requested status to said video source application, and accompanying said returned requested status with a verification key, generated using said symmetric ciphering/deciphering process and employing said first basis value, to allow said video source application to determine whether to trust said returned status.

22. The method of claim 21, wherein said method further comprises said video hardware interface further accompanying said returned status with a selection key for the video source application to use to independently generate its own copy of an authentication key for use to independently generate its own copy of said verification key.

23. The method of claim 21, wherein said generation of said verification key comprises said video hardware interface generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video source application.

24. The method of claim 21, wherein said generation of said verification key comprises said video hardware interface applying a one way function to at least a first selected subset of said first basis value using an authentication key.

25. The method of claim 24, wherein said generation of said verification key further comprises said video hardware interface applying said one way function to a selection key said video hardware interface received from said video sink device for use by said video hardware interface to authenticate said video sink device, using the result of said first application of the one-way function.

26. The method of claim 25, wherein said generation of said verification key further comprises said video hardware interface applying said one way function to at least a second selected subset of said first basis value using the result of said second application of the one-way function.

27. The method of claim 25, wherein said generation of said verification key further comprises said video hardware interface applying said one way function to at least said status using the result of said second application of the one-way function.

28. The method of claim 21, wherein said method further comprises

said video hardware interface receiving from said video source application request for a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to said external video sink device, said secret request being also supplemented with a second basis value to said symmetric ciphering/deciphering process; and

said video hardware interface returning said requested secret in a ciphered form to said video source application, the secret having been ciphered by a ciphering key generated using said symmetric ciphering/deciphering process and employing said second basis value.

29. The method of claim 28, wherein said method further comprises said video hardware interface receiving from said video source application a selection key supplementing said secret request for the video hardware interface to use to generate an authentication key for use in said symmetric ciphering/deciphering process.

30. The method of claim 28, wherein said generation of said ciphering key comprises said video hardware interface generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video source application.

31. The method of claim 28, wherein said generation of said ciphering key comprises said video hardware interface applying a one way function to at least a first selected subset of said second basis value using an authentication key.

32. The method of claim 31, wherein said generation of said ciphering key further comprises said video hardware interface applying said one way function to at least a second selected subset of said second basis value using the result of said first application of the one-way function.

33. In a video source device, a method comprising

a video hardware interface receiving from a video source application request for a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to an external video sink device, said secret request being supplemented with a basis value to a symmetric ciphering/deciphering process; and

said video hardware interface returning said requested secret in a ciphered form to said video source application, the secret having been ciphered by a ciphering key generated using said symmetric ciphering/deciphering process and employing said basis value.

34. The method of claim 33, wherein said method further comprises said video hardware interface receiving from said video source application a selection key supplementing said secret request for the video hardware interface to use to generate an authentication key for use in said symmetric ciphering/deciphering process.

35. The method of claim 33, wherein said generation of said ciphering key comprises said video hardware interface generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video source application.

36. The method of claim 33, wherein said generation of said ciphering key comprises said video hardware interface applying a one way function to at least a first selected subset of said basis value using an authentication key.

37. The method of claim 36, wherein said generation of said ciphering key further comprises said video hardware interface applying said one way function to at least a second selected subset of said basis value using the result of said first application of the one-way function.

38. An article of manufacture comprising:

a storage medium having stored therein a plurality of programming instructions implementing a video source application that requests from a video hardware interface status with respect to a link linking said video source device to an external video sink device, and supplements said status request with a basis value to a symmetric ciphering/deciphering process, when the programming instructions are executed by a processor, the video source application, upon receiving from said video hardware interface said requested status and a verification key generated using said symmetric ciphering/deciphering process and employing said basis value, further verifies the correctness of said verification key to determine whether to trust said provided status.

39. The article of manufacture of claim 38, wherein as part of said verification of the correctness of the received verification key, said video source application independently generates its own copy of an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

40. The article of manufacture of claim 38, wherein as part of said verification of the correctness of the received verification key, said video source application applies a one way function to at least a first selected subset of said basis value

provided to said video hardware interface using an independently generated copy of an authentication key.

41. An article of manufacture comprising:

a storage medium having stored therein a plurality of programming instructions implementing a video source application that requests from a video hardware interface a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to an external video sink device, and supplements said secret request with a basis value to said symmetric ciphering/deciphering process, when the programming instructions are executed by a processor, the video source application, upon receiving from said video hardware interface said requested secret in a ciphered form, having been ciphered using a ciphering key generated using said symmetric ciphering/deciphering process and employing said basis value, further deciphers said ciphered secret using an independently generated copy of said ciphering key.

42. The article of manufacture of claim 41, wherein said video source application independently generates its own copy of said ciphering key, including generation of an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

43. The article of manufacture of claim 41, wherein said video source application independently generates its own copy of said ciphering key, including application of a one way function to at least a first selected subset of said basis value provided to said video hardware interface, using an independently generated copy of an authentication key.

44. An apparatus comprising:

a video hardware interface equipped to securely transmit digital video to an external video sink device coupled to said apparatus by way of said video hardware interface;

a storage medium having stored therein a plurality of programming instructions implementing a video source application that requests from said video hardware interface status with respect to said coupling between said video hardware interface and said external video sink device, and supplements said status request with a basis value to a symmetric ciphering/deciphering process, when the programming instructions are executed, the video source application, upon receiving from said video hardware interface said requested status and a verification key, generated using said symmetric ciphering/deciphering process and employing said basis value, further verifies the correctness of said verification key to determine whether to trust said provided status; and

a processor coupled to said storage medium and said video hardware interface to execute said programming instructions.

45. The apparatus of claim 44, wherein said video source application independently generates its own copy of the verification key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface, for use to verify the correctness of the received verification key.

46. The apparatus of claim 44, wherein as part of said verification of the correctness of the received verification key, said video source application applies a one way function to at least a first selected subset of said basis value provided to

said video hardware interface using an independently generated copy of an authentication key.

47. An apparatus comprising:

a video hardware interface equipped to securely transmit digital video to an external video sink device coupled to said apparatus by way of said video hardware interface;

a storage medium having stored therein a plurality of programming instructions implementing a video source application that requests from said video hardware interface a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to said external video sink device, and supplements said secret request with a basis value to said symmetric ciphering/deciphering process, when the programming instructions are executed, the video source application, upon receiving from said video hardware interface said requested secret in a ciphered form, having been ciphered using a ciphering key generated using said symmetric ciphering/deciphering process and employing said basis value, further deciphers said ciphered secret using an independently generated copy of said ciphering key; and

a processor coupled to said storage medium and said video hardware interface to execute said programming instructions.

48. The apparatus of claim 47, wherein said video source application independently generates its own copy of said ciphering key, including generation of an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

49. The apparatus of claim 47, wherein said video source application independently generates its own copy of said ciphering key, including application of a one way function to at least a first selected subset of said basis value provided to said video hardware interface using an independently generated copy of an authentication key.